CLAIMS

What is claimed is:

1. A method of binary instrumentation comprising:

allocating a contiguous memory region;

filling the memory region with at least one copy of an interceptor function;

initializing a first data structure with at least a starting address, length of the allocated memory region, and a reference to a second data structure;

storing an address of an original function in a current element of the second data structure upon request for instrumentation; and

providing a starting address of a copy of the interceptor function upon request for instrumentation.

2. The method of claim 1, wherein allocating a memory region, filling the memory region, and initializing the first data structure are performed upon an initial request for instrumentation.

3. The method of claim 1, wherein allocating a memory region, filling the memory region, and initializing the first data structure are performed if all interceptor function copies of currently allocated memory regions are associated with previous requests for instrumentation.

4. The method of claim 1, further comprising duplicating the first data structure to associate each new copy of the first data structure with each newly allocated memory region.

5. The method of claim 1, wherein the second data structure comprises elements to store addresses of original functions instrumentation was requested for.

6. The method of claim 1, further comprising maintaining the current element of the second data structure to establish a correspondence between the original function and a provided address of an interceptor function copy.

7. The method of claim 6, further comprising selecting a next successive element of the second data structure as the current element for each new request for instrumentation.

8. The method of claim 1, wherein a reference to the second data structure comprises at least one of a memory address of and an index to the second data structure.

9. The method of claim 1, wherein the starting address of a copy of the interceptor function is provided in a direct correspondence with the current element of the second data structure.

10. The method of claim 1, wherein the interceptor function comprises

obtaining an address being currently executed;

retrieving, from a corresponding copy of the first data structure, the starting address of a memory region that contains the address being currently executed;

fetching the reference to the second data structure from the copy of the first data structure;

computing an index to the second data structure as the fetched reference to the second data structure added to the difference between the address being currently executed and the retrieved starting address, the difference divided by the size of the interceptor function; and

reading, from the second data structure indexed with the computed index, the address of an original function to pass control to.

11. An article comprising: a machine accessible medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for binary instrumentation by:

allocating a contiguous memory region;

filling the memory region with at least one copy of an interceptor function;

initializing a first data structure with at least a starting address, length of the allocated memory region, and a reference to a second data structure;

storing an address of an original function in a current element of the second data structure upon request for instrumentation; and

providing a starting address of a copy of the interceptor function upon request for instrumentation.

12. The article of claim 11, wherein instructions for allocating a memory region, filling the memory region, and initializing the first data structure are executed upon initial request for instrumentation.

13. The article of claim 11, wherein instructions for allocating a memory region, filling the memory region, and initializing the first data structure are executed if all interceptor function copies of currently allocated memory regions are associated with previous requests for instrumentation.

14. The article of claim 11, further comprising instructions for duplicating the first data structure to associate each new copy of the first data structure with each newly allocated memory region.

15. The article of claim 11, wherein the second data structure comprises elements to store addresses of original functions instrumentation was requested for.

16. The article of claim 11, further comprising instructions for maintaining the current element of the second data structure to establish a correspondence between the original function and a provided address of an interceptor function copy.

17. The article of claim 16, further comprising instructions for selecting a next successive element of the second data structure as the current element for each new request for

instrumentation.

18. The article of claim 11, wherein a reference to the second data structure comprises at least one of a memory address of and an index to the second data structure.

19. The article of claim 11, wherein the starting address of a copy of the interceptor function is provided in a direct correspondence with the current element of the second data structure.

20. The article of claim 11, wherein interceptor function comprises instructions for obtaining an address being currently executed;

retrieving, from a corresponding copy of the first data structure, the starting address of a memory region that contains the address being currently executed;

fetching the reference to the second data structure from said copy of the first data structure;

computing an index to the second data structure as the fetched reference to the second data structure added to the difference between the address being currently executed and the retrieved starting address, said difference divided by the size of the interceptor function; and

reading, from the second data structure indexed with the computed index, the address of an original function to pass control to.

21. A system that performs binary instrumentation, comprising:

a plurality of copies of an interceptor function; and

an instrumenting module to allocate a contiguous memory region,

to fill said memory region with the copies of the interceptor function, to initialize a first data structure with at least a starting address, length of the allocated memory region, and a reference to a second data structure, to store an address of an original function in a current element of the second data structure upon request for instrumentation, and to provide a starting address of a copy of the interceptor function upon request for instrumentation.

22. The system of claim 21, wherein the instrumenting module is executed upon an initial request for instrumentation.

23. The system of claim 21, wherein the instrumenting module is executed if all interceptor function copies of currently allocated memory regions are associated with previous requests for instrumentation.

24. The system of claim 21, wherein the instrumenting module duplicates the first data structure to associate each new copy of the first data structure with each newly allocated memory region.

25. The system of claim 21, wherein the second data structure comprises elements to store addresses of original functions instrumentation was requested for.

26. The system of claim 21, wherein the instrumenting module maintains the current element of the second data structure to establish a correspondence between the original function and a provided address of an interceptor function copy.

27. The system of claim 26, wherein the instrumenting module selects a next successive element of the second data structure as the current element for each new request for instrumentation.

28. The system of claim 21, wherein reference to the second data structure comprises at least one of a memory address of and an index to the second data structure.

29. The system of claim 21, wherein the starting address of a copy of the interceptor function is provided in a direct correspondence with the current element of the second data structure.

30. The system of claim 21, wherein the interceptor function is adapted to

obtain an address being currently executed;

retrieve from a corresponding copy of the first data structure the starting address of a memory region that contains the address being currently executed;

fetch the reference to the second data structure from said copy of the first data structure;

compute an index to the second data structure as the fetched reference to the second data structure added to the difference between the address being currently executed and the retrieved starting address, said difference divided by the size of the interceptor function; and

read, from the second data structure indexed with the computed index, the address of an original function to pass control to.